COMMONWEALTH OF MASSACHUSETTS

DEPARTMENT OF TELECOMMUNICATIONS AND ENERGY

Investigation into the Collocation Security Policies of Verizon New England Inc. d/b/a Verizon Massachusetts	)	D.T.E. 02-8

REPLY BRIEF OF ALLEGIANCE TELECOM OF MASSACHUSETTS, INC.

INTRODUCTION

Verizon's initial brief, like the evidence it presented at the hearing, does not demonstrate that any of the colocation security "fixes" it proposes, most especially eliminating physical colocation from certain unidentified "critical" central offices, is necessary to protect its network from harm caused by terrorists or other carriers. The security measures that Verizon has in place, including card reader access systems, security cameras, the use of separate and secure space for physical collocation, requiring background checks of CLEC personnel having access to central offices and the issuance of ID badges to such CLEC personnel have thus far proved effective in averting network outages in Massachusetts caused by CLECs. Verizon has failed to make the case that prohibiting physical collocation in any central office is necessary to safeguard the network.

I. Verizon Relies on the Wrong Standard of Review

The Department opened this investigation pursuant to G.L. c. 159, §§ 12 and 16 to assess the adequacy of Verizon's security practices. In response, Verizon has proposed a series of new

colocation rules, and asks the Department to find that the proposal "appropriately addresses the legitimate security concerns raised in its Order, and reflects `just, reasonable, safe, adequate and proper regulations and practices' under Section 16 of Chapter 159 of the Massachusetts General Laws." Verizon Brief at 6. Verizon has omitted the first half of the standard of review the Department must apply in this case. Section 16 of G.L. c. 159 states:

> **If the department is of [the] opinion, after a hearing had upon its own motion or upon complaint, that the regulations, practices, equipment, appliances or service of any common carrier are unjust, unreasonable, unsafe, improper or inadequate**, the department shall determine the just, reasonable, safe, adequate and proper regulations and practices thereafter to be in force and to be observed, and the equipment, appliances and service thereafter to be used, and shall fix and prescribe the same by order to be served upon every common carrier to be bound thereby (emphasis added).

The Department recognized this standard in its Order, which states that this investigation will determine "whether Verizon's security policies meet the statutory standard for `just, reasonable, safe, adequate and proper regulations and practices.' G.L. c. 159, § 16." Thus, the Department cannot, as Verizon implies, merely examine Verizon's proposed new colocation rules and conclude that those rules meet the requirements of Section 16. To even consider any proposal by a party to this case, the Department must first make findings, supported by substantial evidence, that Verizon's "regulations, practices, equipment, appliances or service . . . are unjust, unreasonable, unsafe, improper or inadequate." *See, e.g., Penn Central Company v. Department of Public Utilities*, 356 Mass. 478 (1969); *Holyoke Street Railway Company v. Department of Public Utilities*, 347 Mass. 440 (1964). Verizon has focused on the second half of the Section 16 standard of review (trying to establish that its new proposal is just, reasonable, safe, adequate and proper) while virtually ignoring the first half (the status of its existing security measures).

The Department cannot consider Verizon's enhanced security proposals without first making an explicit finding that Verizon's current practices violate Section 16, especially when those proposals could have such a detrimental impact on CLECs. By failing to offer evidence that its current practices are "unjust, unsafe, improper, or inadequate," Verizon has put before the Department no basis on which the Department can move to the second stage of the inquiry.[1]

Verizon argues in its brief that its proposal is "consistent with the Department's previous decision in D.T.E. 98-21 (*Covad Communications Company*), which rejected Covad's proposal for unsecured cageless collocation arrangements in Massachusetts." Verizon brief at 31. Yet "the Department's previous decision in D.T.E. 98-21" was *reversed* by the Department itself:

> In response to the Advanced Services Order and space utilization concerns in Massachusetts central offices, the Department in 1999 reversed its findings in Covad/Bell Atlantic Arbitration Order and required Verizon to submit tariff revisions that included the alternative collocation arrangements, including cageless collocation, required by the FCC in the Advanced Services Order. Teleport Petition, D.T.E. 98-58, at 26 n.20 (1999).

Vote and Order at 4.

Moreover, Verizon ignores the most significant legal development that bears directly on the standard for cageless colocation that was adopted by the Department in D.T.E. 98-58. In *G.T.E. Services v. Federal Communications Commission*, the D.C. Circuit upheld the FCC's requirement that ILECs offer cageless colocation to CLECs, but vacated and remanded part of the *Advanced Services Order* to the FCC for further consideration of the rules that should govern cageless colocation. Those rules, which have already been discussed at length in the initial briefs

[1] Verizon also suggests another standard of review, that its proposed security measures should be judged not against applicable Department precedent and FCC regulations, but against the security measures employed by CLECs. Verizon Brief at 58-59. In making this argument, Verizon yet again simply ignores the law. ILECs have a statutory obligation to allow CLECs to colocate in ILEC facilities, not vice versa. 47 U.S.C. § 251(c).

of Allegiance and other CLECs, were promulgated by the FCC in its *Collocation Remand Order*, and were the subject of petitions for review filed by Verizon and other ILECs. In its panel testimony, Verizon noted its appeal of the regulations promulgated in the *Collocation Remand Order*, and even set forth its arguments on appeal as support for its request that the Department ignore the FCC's regulations in fashioning new colocation rules for Massachusetts. Exh. VZ-MA-1, at 16-17.

Subsequent to the hearing, Verizon's petition for review and those of the other ILECs were denied and the FCC's rules remain in effect. *Verizon et al. v. FCC et al*, 292 F.3d 903 (D.C. Cir. 2002). Rather than concede its loss and work toward identifying any legitimate security concerns that could and should be addressed by the industry as a whole, Verizon continues to re-litigate the same case against physical colocation that it has lost before Congress, the FCC, the Federal courts, and the Department. Despite the fact that the federal Communications Act and the FCC's regulations guarantee CLECs the right to physically colocate in Verizon's central offices, Verizon continues to argue that "COs were not, however, designed to accommodate or house equipment used by multiple carriers," and that "the presence of all types of physical collocation inherently compromises Verizon MA's ability to protect its network from *within* the CO," and that this situation warrants a significant roll-back of CLECs' right to physical colocation guaranteed by the Act. Verizon Brief at 17 (emphasis in original). The Department should recognize that Verizon has presented these arguments in great detail in every proceeding before every tribunal that has considered the issue of physical colocation. These arguments have nothing to do with September 11th, or any new security threat identified as a result of that tragedy, and Verizon does not even attempt to tie its proposal to any such legitimate security concern. These are the same arguments that Verizon has been making,

unsuccessfully, since 1996, warmed over and presented yet again, with a national catastrophe as the newly-adopted backdrop.

II. The Evidence Cited by Verizon Would Support Neither a Finding by the Department that Verizon's Current Security Practices are "Unjust, Unsafe, Improper, or Inadequate," Nor a Finding that Verizon's Proposal is "Just, Safe, Adequate, and Proper."

The record does not support Verizon's underlying thesis that its current security practices are "unjust, unsafe, improper, or inadequate" only because of the presence of CLECs in its central offices, and that the only way to remedy this situation is to systematically limit or exclude that CLEC presence. For this reason, the Department should deny Verizon's requests for relief.

A. A Connection Between CLEC "Foot Traffic" and Network Security Concerns Remains Unproven.

Despite Verizon's efforts to establish that it is "reasonable and necessary" to restrict "'foot traffic' or access by colocators in areas where Verizon MA's facilities and equipment are collocated" (Verizon Brief at 14), the record in this case instead demonstrates that it is not CLEC "foot traffic", but Verizon "foot traffic", that has been the cause of reported CO incidents and network outages.

First, Verizon has never experienced a network-affecting incident caused by CLEC personnel. In its response to information request AG-VZ-1-1, Verizon produced incident reports prepared by two of its departments – the Collocation Care Center and the Security Department. Not a single one of these reports involves a CLEC-caused network-affecting incident. In contrast, from 1999 through the present, Verizon employees or vendors have caused six network outages.[2] RR-DTE-VZ-1, Att. 1.

[2] The seventh outage reported to the FCC was caused by a water company not having access to the COs. Id.

Second, these incident reports also include no evidence of any non-network-affecting incident caused by CLEC personnel. While these reports show 28 security breaches at Verizon COs, seven (or one-fourth) of the breaches involved picketing or vandalism associated with Verizon employees' August 2000 work stoppage, and almost all of the other breaches involved theft or damage to CLEC equipment and cages – incidents where Verizon was unable to identify the party responsible for the breach. RR-DTE-VZ-2.

Verizon's position that CLEC "foot traffic" renders its security measures "unfair, unsafe, improper, or inadequate" is simply not supported by any factual evidence. Rather, Verizon must rely on opinion and argument, unsupported by evidence of any actual threats to its network, that "the advent of physical collocation" has resulted in an "unfair, unjust, improper, or inadequate" security situation in its COs. Id.

For example, Verizon spends three pages of its brief discussing "security breaches" documented in Exh. AG-VZ-1-1. Verizon Brief at 21-23. This discussion, however, lumps together incidents from other states, without distinguishing one from another, and without proof of CLEC involvement, in order to exaggerate the threat allegedly posed by CLECs. Verizon concludes this discussion by stating:

> Although those *reported* security violations may not be all-inclusive, they demonstrate the types of security breaches that occur with "greater" foot traffic within the CO and the harm or damage that can result to Verizon's and/or collocators' equipment or facilities. Tr. 63, 73, 376-76. This includes, in some cases, service outages affecting thousands of customers. *Id.*

Verizon Brief at 22 (italics in original).

This statement gives the impression that CLECs have, in fact, caused "service outages affecting thousands of customers" in Verizon's territory, perhaps even in Massachusetts, which the evidence simply does not show. As stated above, Verizon itself admits that there is not one

documented "security breach" in Massachusetts that was proven to be caused by CLEC personnel, and there is no instance of a CLEC causing any outage in Massachusetts, much less one "affecting thousands of customers." The only incident Verizon cites for this proposition is from the State of Washington which, as described in the initial brief of Covad Communications, remains in dispute. Covad Brief at 6-7.

B. Verizon's Attempts to Impugn the Motivations and Performance of CLEC Personnel In General Find No Support in the Record.

Even though the record shows that it has been Verizon employees and vendors, rather than CLECs, that have been responsible for network disruptions, Verizon nonetheless maintains that its security efforts are hampered by its inability to dismiss or discipline CLEC employees. Verizon Brief at 28, 29, 47. This particular argument is a true red herring. First, there is evidence in the record that Verizon employees and vendors have been responsible for both network-affecting and non-network affecting incidents, yet Verizon admits that it "has not terminated or undertaken to terminate any of its CO technicians or equipment installation technicians for accidentally causing damage within or to Verizon MA's COs" during the period of reported incidents. Exh. AL-VZ-16, at 2. It is somewhat baffling that even where Verizon could point to no security breaches associated with activities of a colocator's personnel, Verizon still views itself as hampered with respect to ensuring security at its colocated COs because it has no authority to dismiss or discipline CLEC employees *who have never caused an incident*.

Second, even if there were evidence that CLECs were responsible for some CO incidents – which there decidedly is not – there is no basis in the record (or in logic, for that matter) for Verizon to presume that CLECs would not discipline their employees for security breaches and that such discipline would not be just as effective as anything Verizon might want to undertake.

Verizon's unsubstantiated presumption also fails to take into account that CLECs, as well as Verizon have a vested interest in maintaining a fully functioning telecommunications network.

Further, Verizon's argument continues to ignore the fact that Verizon can effectively "discipline" CLEC employees for security violations. While Verizon cannot terminate the employment of CLEC personnel who violate security procedures, Verizon can impose disciplinary measures up to and including "termination of all access privileges." Verizon Brief at 42, n. 53. Such a termination of access privileges would have a drastic impact on an employee's value to his or her employer and, thus, provides a strong incentive to follow the rules. Verizon's ability to exclude a CLEC employee from its COs provides a strong incentive for CLEC personnel to adhere to the security rules and regulations. See Exh. AL-VZ-1-16.

Verizon also continues to argue that its colocation security proposal is necessary because of CLECs' failure to "return access credentials that are no longer required" (Verizon Brief at 45). This argument is not persuasive for a number of reasons. First, as is the case with Verizon's argument regarding its inability to discipline CLEC employees who breach security, Verizon is failing "to see the forest for the trees." Here, once again, Verizon hammers on one non-critical point and ignores the clear evidence that CLECs were not responsible for either network-affecting or non-network-affecting incidents in recent years.

Second, Verizon provides only anecdotal evidence of the alleged problem with unreturned credentials. In fact, in response to a discovery request regarding the magnitude of this alleged problem, Verizon itself stated that "[T]he number of access cards issued to CLECs in

Massachusetts is not readily available"; and that "Verizon MA cannot not [sic] track the number of expired (*i.e.,* non-renewed) access cards that were lost or not returned" Exh. AL-VZ-1-6.[3]

Third, and quite significantly, Verizon in its brief mischaracterizes the testimony of Allegiance's witness on this very issue. Here, Verizon notes only that some parties, including Allegiance, seldom follow the procedure requiring the return to Verizon of access credentials (Verizon Brief at 45, *citing* Tr. 411), omitting a critical piece of testimony, *i.e.,* that Allegiance destroys the access cards of personnel that leave its employ (Tr. 411). And, while Allegiance does not contend that destroying rather than returning to Verizon access credentials of ex-employees is in perfect compliance with Verizon's website requirements, the effect is the same and the practice is fully consistent with Verizon's and Allegiance's security interests.

Moreover, Allegiance's practice of destroying the access credentials of former employees appears to be consistent with Verizon's own practices in that regard. In its brief, Verizon offers the following footnote:

> By contrast, Verizon MA confiscates ID badges and access cards of its former employees and contractors upon termination of their employment. Tr. 730. This prevents them from gaining unauthorized access after their employment has ended.

(Verizon Brief at 45, n.56). Allegiance likewise confiscates and then destroys ID badges and access cards of its former employees which prevents them from gaining unauthorized access to COs after their employment has ended.

[3] Other statements of alleged problems with "unauthorized use" of access cards also have no citation to the record. Verizon Brief at 27. Presumably, if Verizon had even one documented case in which a CLEC employee was found in a CO without proper identification, or a non-CLEC trespasser gained access to a CO by using a CLEC employee's access card or key, that case would have been front and center in its testimony and brief.

C. Verizon's Failure to Produce Evidence of the Current Status of Security Measures in its COs Remains Unexplained.

As discussed in Allegiance's initial brief, Verizon admits that it has not conducted any CO-specific risk assessments that it relied upon in making its security proposal to the Department. Allegiance Brief at 6. In its brief, Verizon attempts to defend its inaction using the concept of a security "baseline," as discussed at page 23, note 35:

> First, a per CO risk assessment is not required because Verizon MA's collocation security proposal outlines an appropriate *baseline* plan for enhancing security in *all* COs. Second, the typical risk assessment examines whether a building is located in a high crime area to determine relative risk. The basic premise of such risk assessments may no longer be sufficient given the events of September 11th. Tr. 28. Third, it would be premature to perform risk assessments on "critical" offices because the Department has not yet approved the concept – nor designated which offices would qualify based on specific criteria. Tr. 63. Finally, it is ironic that parties, such as AT&T, have not completed risk assessments for their Massachusetts locations, given their position on this matter. Tr. 439.

The argument that Verizon cannot perform a risk assessment at so-called "critical" COs because neither the criteria to identify those COs nor the COs that meet the criteria have been approved by the Department is indicative of Verizon's entire approach to this case. While Verizon details a parade of horribles that *could* occur at a CO, it has failed to come forward with any solid evidence that such a parade of horribles is more likely to occur because CLECs are physically colocated in the COs. Verizon is essentially saying that it would be useless to study the actual risk present at *any* CO because the Department has not yet determined which, if any, COs might be critical. This argument appears to ignore Mr. Craft's testimony that one should perform a risk assessment at a facility *before* determining what level of security is appropriate for that facility. Tr. 24.

Verizon contends that it is ironic that CLECs criticize it for not conducting risk assessments when CLECs themselves may not have conducted risk assessments. Ironic or not,

Verizon's contention is beside the point. It is *Verizon's* security practices that are the subject of the Department's investigation here, not the CLECs' security practices. Verizon's failure to undertake risk assessments at its COs just makes it that much more difficult for the Department to determine whether Verizon's *current* security practices are "unfair, unsafe, improper, or inadequate."

D. Verizon's Advocacy of Virtual Colocation Cannot Blunt Its Inherently Anti-Competitive Characteristics.

The initial briefs of the CLECs in this case amply demonstrate the inherent inferiority of virtual colocation to physical colocation, and those arguments will not be repeated here. Verizon's brief does nothing to counter the unanimous view of the CLECs that virtual colocation is not an acceptable arrangement for their business purposes in Massachusetts. The fact that the Act requires physical colocation, and that virtual colocation can be substituted only under very narrow conditions, is a strong indication that Congress itself saw physical as superior to virtual colocation.

In considering the various arguments presented regarding virtual colocation, the Department should keep in mind that, regardless of how well Verizon promises or even delivers service in a virtual arrangement, the substitution of virtual for physical colocation cannot be accomplished consistent with the Act. The Department has distinguished itself over the years by continually taking steps to effectively and efficiently open the monopoly local telephone market to competition. The Department should continue on that path and resist Verizon's pleas to solidify its monopoly position by depriving its competitors of the collocation rights to which they are entitled under federal law.

CONCLUSION

The record in this case supports only these conclusions: First, CLECs share Verizon's interest in maintaining secure COs and a properly functioning telecommunications network. Second, CLECs and their personnel have acted responsibly in maintaining and accessing their physical colocation arrangements here in Massachusetts and, as a result, security in Verizon COs is generally "just, reasonable, safe, adequate and proper." If it could be improved, (and there is always room for improvement where humans are involved), such improvements should focus on what is lacking in Verizon's current practices and procedures rather than on excluding CLECs from access to their colocated equipment.

Respectfully submitted,

ALLEGIANCE TELECOM OF MASSACHUSETTS, INC.

By its attorneys

_____

Robert D. Shapiro
Christopher H. Kallaher
Rubin and Rudman LLP
50 Rowes Wharf
Boston, MA 02110
Tel. No. (617) 330-7000

_____

Mary C. Albert
Vice President, Regulatory and Interconnection
Allegiance Telecom, Inc.
1919 M Street, N.W., Suite 420
Washington, DC 20036

Dated: August 23, 2002